Kyberprevence

Strategický plán proaktivního hodnocení rizik a zabezpečení dat

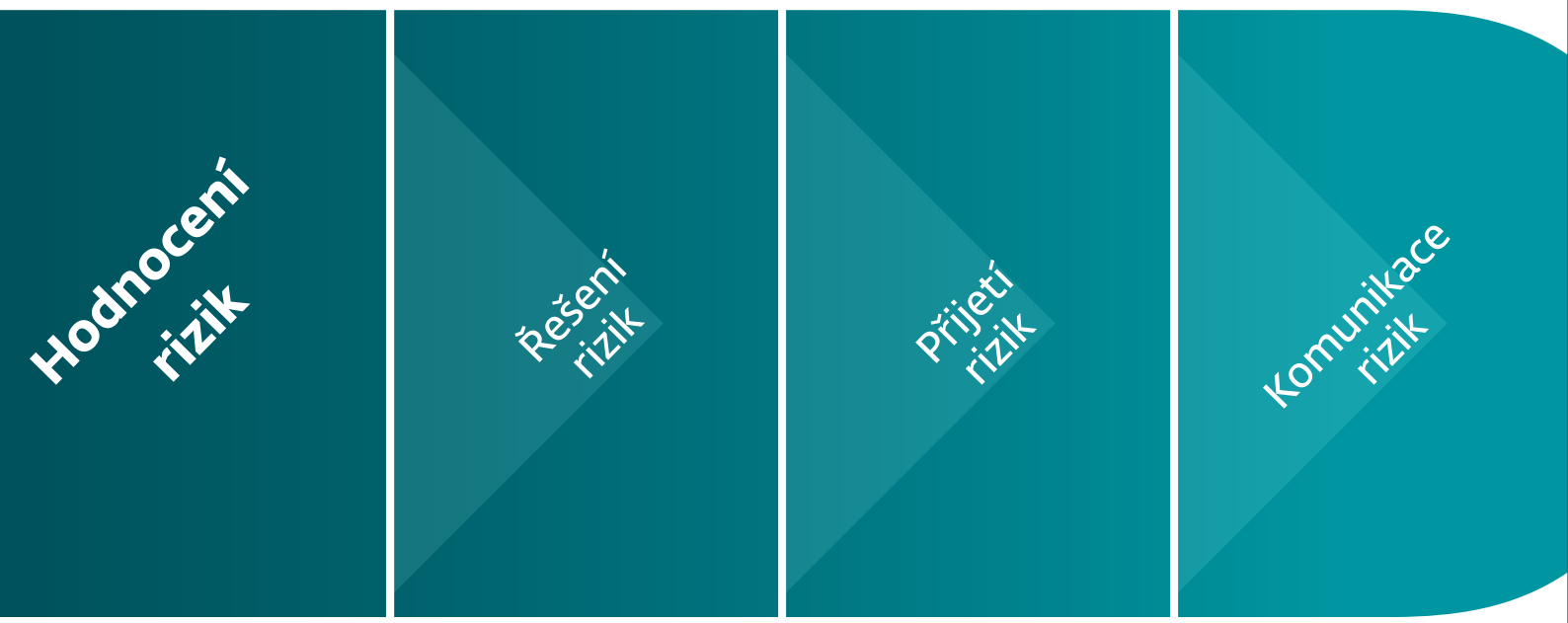
Digital Security
Progress. Protected.

Přístup založený na posouzení rizik nejenže umožňuje organizacím zavést vhodné kontrolní mechanismy přizpůsobené konkrétním hrozbám, ale také klade **důraz na prevenci jako strategickou prioritu**. Zařazením preventivních opatření do počáteční fáze řízení rizik bezpečnosti mohou organizace proaktivně řešit zranitelnosti a zmírňovat potenciální hrozby.

Proces hodnocení rizik zahrnuje důkladnou **identifikaci aktiv, analýzu hrozeb a posouzení zranitelných míst společnosti**, aby společnost dosáhla komplexního porozumění potenciálním rizikům. Tento krok je klíčový k tomu, aby IT manažeři mohli přijímat informovaná rozhodnutí ohledně zmírnění, postoupení, zamezení nebo přijetí rizik. Vyžaduje také jasnou komunikaci se zúčastněnými stranami o jejich proaktivní roli při řízení a prevenci těchto rizik.

Klíčové je pochopení drobných rozdílů u rizik spojených se zabezpečením dat, zejména identifikací operací zpracování dat a vyhodnocení jejich potenciálních dopadů na podnikání. To vytváří předpoklady pro určení relevantních hrozeb, pravděpodobnosti, s jakou se s nimi lze setkat, a vyhodnocení rizik, aby bylo zajištěno účinné zabezpečení dat s využitím organizačních i technických kontrol v rámci ucelené strategie řízení bezpečnosti.

Čtyři klíčové fáze řízení rizik bezpečnosti



Fáze 1: Hodnocení rizik

První fází je posouzení rizik. Existuje mnoho metodik hodnocení rizik s různou úrovní nákladů a složitosti. Základní proces se skládá z následujících částí:

- **Identifikace aktiv: I**dentifikujte všechna aktiva v organizaci (hmotná i nehmotná), která je třeba chránit, a určete jejich kvantitativní (např. náklady nebo příspěvek k výnosům) a/nebo kvalitativní hodnotu (např. relativní důležitost).
- **Analýza hrozeb:** Definujte možné nepříznivé přírodní a/nebo člověkem způsobené jevy nebo události, které mohou mít potenciální dopad na společnost. Určete jejich pravděpodobnost a četnost výskytu.
- **Posouzení zranitelností:** Určete, jaká ochranná a/nebo kontrolní opatření aktiv chybí nebo jsou slabá a činí tím hrozby potenciálně škodlivějšími, nákladnějšími, pravděpodobnějšími nebo častějšími.

Další klíčové fáze

Řešení rizik: Po vyhodnocení rizik mají IT správci několik možností:

- **Zmírnění rizik**, které snižuje dopad nebo pravděpodobnost hrozby prostřednictvím politik a kontrolních mechanismů;
- **Postoupení rizik**, kdy je riziko převedeno na třetí stranu, například pojišťovnu;
- **Zamezení rizik**, které zahrnuje úplnou eliminaci rizika prostřednictvím modernizace, likvidace aktiva nebo zastavení činnosti, která riziko způsobuje.

Přijetí rizik: Jedná se o formální vedením schválená opatření k ošetření rizik a přijetí jakéhokoli zbytkového rizika, které nelze více omezit, postoupit nebo se mu vyhnout.

Komunikace rizik: Zúčastněné strany musí být informovány o všech přijatých rozhodnutích o řešení a/nebo přijetí rizika, včetně jejich jednotlivých rolích a odpovědností týkajících se konkrétních rizik.

Porozumění procesu hodnocení rizik

Hodnocení rizik je první fází procesu řízení rizik. Hodnocení rizik se skládá z identifikace aktiv, analýzy hrozeb a posouzení zranitelností.

Posouzení rizik zabezpečení dat zahrnuje:

- Identifikaci operací zpracování dat (určení, jak a kde jsou ve vaší firmě datová aktiva používána).
- Určení potenciálního dopadu na podnikání (pokud dojde k ohrožení vašich dat).
- Identifikaci možných hrozeb a vyhodnocení jejich pravděpodobnosti výskytu (včetně četnosti).
- Vyhodnocení rizik (za účelem posouzení, jaká bezpečnostní opatření nebo kontrolní mechanismy musíte ve firmě zavést k ochraně údajů).

Krok 1: Identifikace operací zpracování dat

Data v organizaci mají různé rizikové profily, a to nejen na základě typu dat, ale také kvůli způsobu, jakým jsou data v organizaci využívána. Při zahájení procesu hodnocení rizik je tedy důležité **pochopit, jakým způsobem jsou data ve vaší firmě zpracovávána**. Například v typickém malém a středním podniku můžete mít některé z následujících typů operací zpracování dat:

- **Lidské zdroje**: správa mezd zaměstnanců, nábor a péče o zaměstnance, záznamy o školeních, disciplinární řízení a hodnocení výkonnosti.
- **Správa zákazníků, dodavatelů a marketing**: informace o zákaznících, objednávky, faktury, seznamy kontaktů, marketingové a reklamní údaje a smlouvy s dodavateli.
- **Bezpečnost zaměstnanců a fyzická ochrana**: záznamy o přístupu zaměstnanců, záznamy o návštěvách a video-monitorování.

Pro každou operaci zpracování dat zvažte následující:

- Jaké osobní údaje se zpracovávají?
- Jaký je účel zpracování?
- Kde ke zpracování dochází?
- Kdo je za zpracování odpovědný?
- Kdo má k údajům přístup?

Krok 2: Určení potenciálního dopadu na podnikání

Dále je třeba určit potenciální dopad narušení nebo kompromitace dat na vaši společnost. Narušení nebo kompromitace může mít vliv na důvěrnost (například neoprávněný přístup) dat, integritu dat (například neoprávněná modifikace) nebo dostupnost dat (například při útoku ransomwarem).

Organizace musí chránit důvěrnost, integritu a dostupnost dat. V oblasti zabezpečení informací je tato problematika známá jako C-I-A triáda.

V typickém hodnocení rizik se potenciální dopad daného rizika obvykle vyjadřuje jako škoda pro organizaci, například ztráta nebo zničení fyzického aktiva (například serveru, kopírky nebo vozidla).

Dopad rizika bezpečnosti dat na podnik je podobný jako u jiných rizik, ale může mít také nepřímý vliv. V případě citlivých osobních údajů je přímou obětí člověk, jehož údaje byly narušeny nebo ohroženy. V takových případech může dojít ke krádeži identity nebo finančních aktiv jednotlivce a/nebo k narušení jeho soukromí. Dopad na podnik je méně přímý, ale stále velmi nákladný a může zahrnovat (mimo jiné):

- ztrátu zákazníků a příjmů,
- poškození značky a nepříznivé vztahy s veřejností,
- pokuty od regulačních orgánů a soudní spory,
- oznámení o narušení bezpečnosti,
- forenzní analýzu a obnovu.

Dopad na podnikání lze klasifikovat jako nízký, střední nebo vysoký. Skutečná definice každé z těchto úrovní dopadu je však pro každý podnik jedinečná a měla by zahrnovat jak objektivní (kvantitativní), tak subjektivní (kvalitativní) měřítka.

Krok 3: Identifikace možných hrozeb a vyhodnocení jejich pravděpodobnosti

Hrozbou může být jakákoli událost nebo jev, ať už přírodní, nebo způsobená člověkem, která má potenciál negativně ovlivnit **důvěrnost, integritu nebo dostupnost osobních údajů**. Může se jednat o kybernetické útoky, ztrátu nebo vyzrazení informací, vnitřní hrozby, požáry a záplavy, zemětřesení, hurikán nebo tornádo, občanské nepokoje, pracovní spory a další.

Firmy musí možné **hrozby, které ovlivňují procesy zpracování dat, identifikovat a vyhodnotit pravděpodobnost** (včetně četnosti výskytu) každé z nich. Ujistěte se, že pokrýváte hrozby v dobře definovaných oblastech, včetně hrozeb na straně síťových a technických prostředků (software/hardware), které používáte pro zpracování dat, hrozeb v souvisejících procesech a postupech, hrozeb na straně lidských zdrojů a hrozeb z rozsahu zpracování. U každé identifikované hrozby lze klasifikovat pravděpodobnost stejně jako dopad na podnikání: nízká, střední nebo vysoká.

Krok 4: Vyhodnocení rizika

Jakmile identifikujete všechny operace zpracování dat (a zpracovávaná data), určíte potenciální obchodní dopad jejich narušení nebo kompromitace a identifikujete možné hrozby a pravděpodobnost a četnost jejich výskytu, můžete v**yhodnotit riziko spojené s každou operací** a určit vhodné bezpečnostní a procesní kontroly.

Podle vyhodnocení rizik, tedy pomocí přístupu založeném na posouzení rizik, zaveďte organizační a procesní kontroly, abyste řádně zabezpečili své podnikání a operace zpracování dat.

Organizační a procesní kontroly

Pokud se chcete zaměřit na prevenci, bude to vyžadovat více než jen technická řešení. **Zaveďte administrativní a organizační kontroly**, které zajistí, že technické kontroly budou správně nasazeny, nakonfigurovány a prováděny v souladu s ucelenou strategií řízení bezpečnosti.

Mezi příklady organizačních kontrol patří např.:

- **Soukromé a citlivé osobní údaje**: Aplikujte technické kontroly, jako je šifrování a software na ochranu proti ztrátě dat.
- **Dokumentace a audit dat**: Dokumentujte, proč jsou data shromažďována, jak jsou používána, a jak jsou chráněna.
- **Bezpečnostní zásady**: Jasně definujte jednotlivé role a odpovědnosti související s ochranou osobních údajů.
- **Lidské zdroje**: Zajistěte, aby osobní údaje shromažďované zaměstnanci byly řádně chráněny.
- **Používejte zralostní (maturity) model úrovně bezpečnosti**: Určete možnosti svého zabezpečení v konkrétních oblastech a identifikujte případné mezery mezi tím, kde jste, a tím, kde byste měli být.
- **Školení a testování zaměstnanců**: Zajistěte školení bezpečnosti a testujte zaměstnance, aby si upevnili znalosti.
- **Zavedení ochrany dat již od návrhu a ve výchozím nastavení**: Zaveďte opatření k minimalizaci shromažďování, zpracování a ukládání osobních údajů.

.

My jsme ESET

Proaktivní ochrana.

Eliminujeme způsoby, kterými útočníci mohou proniknout do vaší organizace.

Buďte o krok napřed před známými i nově vznikajícími kybernetickými hrozbami a zaměřte se na prevenci. Bezpečnostní řešení od ESETu efektivně **kombinují umělou inteligenci a odborné znalosti našich expertů.**

Zažijte nejlepší ochranu ve své třídě díky **zpravodajství o hrozbách**, které je již více než 30 let hnacím motorem naší rozsáhlé sítě výzkumných a vývojových poboček vedených **uznávanými specialisty v oboru**. ESET chrání vaši firmu, aby mohla naplno využít potenciál technologií.

ZJISTIT VÍCE

ESET®

Digital Security
Progress. Protected.